4. (Amended) A module as claimed in [any preceding] Claim 1, wherein the at least one certificate is stored externally of said module at a remote location which is derivable from an address stored on said module.

5. (Amended) A module as claimed in [any preceding] Claim 1, wherein the further private key is the manufacturer's private key.

6. (Amended) A module as claimed in [any one of Claims] Claim 1 [to 4], wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key.

7. (Amended) A method of manufacturing a tamper-evident wireless application protocol identity module (WIM) [including] comprising the [steps] step of:

storing a public-private key pair on said module together with a manufacturer certificate signed using a further private key.

10. (Amended) A method according to [Claim 8 or] Claim 9, wherein the manufacturer certificate is created externally of the module.

11. (Amended) A method according to Claim 10 [as appendant to Claim 9], wherein the module is accessed to obtain the public key to facilitate the external creation of the certificate.

12. (Amended) A method as claimed in [any one of Claims] claim 7 [to 11], wherein the further private key is the manufacturer's private key.

13. (Amended) A method as claimed in Claim 9, further comprising [including] the [additional] steps of:

storing an externally created initial management key pair and an initial management certificate signed using the manufacturer's private key on said module[,]; and

storing an internally created manufacturer certificate on said module wherein the further private key is the initial management private key.

14. (Amended) A method of validating a tamper-evident wireless application protocol identity module (WIM) on which

is stored at least one public-private key pair together with a manufacturer certificate signed using a further private key, the method [including] comprising the step of:

querying a public directory to obtain a public key certificate with which to verify the signature generated by the further private key.

15. (Amended) A method of validating the identify of a communication terminal for conducting transactions on the network comprising the steps of:

establishing the identity of a user of the terminal connected to the network[,];

interrogating the terminal to obtain a public key of a public-private key pair stored on the terminal[,];

conforming the authenticity of a certificate signed by the module manufacturer supporting the public key; and

subsequently issuing a further certificate for the public key which certificate is available to support transactions with the terminal over the network.

---

19. (Amended) A method of satisfying an identity module issuer of the provenance of an identify module for use in transactions on a network comprising the steps of: [comprises the issuer]

approving, by the issuer, a manufacturing process of the module manufacturer; [and having]

storing, by the manufacturer, [store] a manufacturer certificate signed securely by the manufacturer on a module produced in accordance with the approved process[, wherein on]; and

upon connection to the network of a terminal containing a module, verifying the signature [is verified] to determine whether it is the manufacturer's signature.

20. (Amended) A method as claimed in Claim 19, wherein the manufacturer certificate is signed using the manufacturer's private key such that on connection to the network a public key certificate is obtained with which to verify the signature.

21. (Amended) A method as claimed in Claim 19 [or Claim 20], wherein the verification of the signature is carried out by the issuer.

22. (Amended) A method as claimed in [an one of Claim] claim 19 [to 21], wherein following successful verification of a signature, a further public key certificate is made

available to support transactions with the terminal, the public key having been stored in the manufacturer certificate.

Please add new claims 23-39 as follows:

-- 23. A module as claimed in Claim 2, further including a certification authority certificate.

24. A module as claimed in Claim 2, wherein the at least one certificate is stored externally of said module at a remote location which is derivable from an address stored on said module.

25. A module as claimed in Claim 3, wherein the at least one certificate is stored externally of said module at a remote location which is derivable from an address stored on said module.

26. A module as claimed in Claim 2, wherein the further private key is the manufacturer's private key.

27. A module as claimed in Claim 3, wherein the further private key is the manufacturer's private key.

28. A module as claimed in Claim 4, wherein the further private key is the manufacturer's private key.

29. A module as claimed in Claim 2, wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key.

30. A module as claimed in Claim 3, wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key.

31. A module as claimed in Claim 4, wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key.

32. A method according to Claim 8, wherein the manufacturer certificate is created externally of the module.

33. A method as claimed in claim 8, wherein the further private key is the manufacturer's private key.

34. A method as claimed in claim 9, wherein the further private key is the manufacturer's private key.

35. A method as claimed in claim 10, wherein the further private key is the manufacturer's private key.

36. A method as claimed in claim 11, wherein the further private key is the manufacturer's private key.

37. A method as claimed in Claim 20, wherein the verification of the signature is carried out by the issuer.

38. A method as claimed in claim 20, wherein following successful verification of a signature, a further public key certificate is made available to support transactions with the terminal, the public key having been stored in the manufacturer certificate.

39. A method as claimed in claim 21, wherein following successful verification of a signature, a further public key certificate is made available to support transactions with the terminal, the public key having been stored in the manufacturer certificate.--